FortiAnalyzer

Application and Risk Analysis - One-Arm

Report Date: 2013-12-23

Data Range: 2013-12-01 00:00 - 2013-12-23 09:10 ART (FAZ local)

FORTINET

Fortinet Inc. All Rights Reserved.

Top Application Users By Bandwidth

This chart provides information about the users who are creating the most network traffic in terms of bandwidth usage. It helps the network manager to identify users that are potentially abusing network usage or creating traffic that does not comply with internal security policies. The following chart displays the top 20 users by bandwidth usage.

Top 20 Users By Bandwidth

User (or IP)	Source IP	Bandwidth (Traffic Out / Traffic In)
192.168.1.44	192.168.1.44	839.26 MB
192.168.1.110	192.168.1.110	12.41 MB
192.168.1.101	192.168.1.101	6.55 MB
67.217.86.241	67.217.86.241	4.92 MB
68.64.21.39	68.64.21.39	4.61 MB
192.168.1.99	192.168.1.99	2.59 MB
192.168.1.123	192.168.1.123	115.51 KB
200.12.41.34	200.12.41.34	67.81 KB
201.17.37.73	201.17.37.73	23.56 KB
98.77.241.150	98.77.241.150	18.62 KB
201.235.142.23	201.235.142.23	16.62 KB
192.168.1.26	192.168.1.26	15.86 KB
181.135.109.254	181.135.109.254	11.51 KB
190.230.127.68	190.230.127.68	9.57 KB
190.22.220.13	190.22.220.13	7.97 KB
181.130.85.19	181.130.85.19	7.92 KB
181.208.245.97	181.208.245.97	7.77 KB
179.4.120.29	179.4.120.29	7.73 KB
213.146.167.32	213.146.167.32	7.40 KB
177.40.197.169	177.40.197.169	6.76 KB

Top Application Users By Sessions

The Top Users In Terms of Sessions section illustrates the quantity of network users who are opening the highest number of connections. This is a critical value because some users could open much more sessions than they are suppose to. Statistics on the amount of sessions a user has opened and the memory space used by these sessions is recorded in the FortiGate. The following chart displays the top 20 users by the number of sessions.

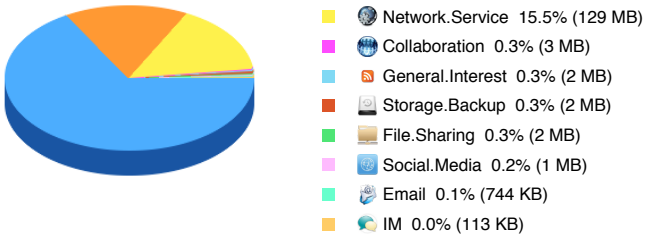
Top 20 User Source By Sessions

User (or IP)	Source IP	Sessions
192.168.1.44	192.168.1.44	52333
192.168.1.110	192.168.1.110	4598
192.168.1.99	192.168.1.99	1428
192.168.1.101	192.168.1.101	669
192.168.1.1	192.168.1.1	190
192.168.1.123	192.168.1.123	103
201.17.37.73	201.17.37.73	59
98.77.241.150	98.77.241.150	45
201.235.142.23	201.235.142.23	42
181.135.109.254	181.135.109.254	30
67.217.86.241	67.217.86.241	25
190.22.220.13	190.22.220.13	23
68.64.21.39	68.64.21.39	23
190.230.127.68	190.230.127.68	22
181.204.25.18	181.204.25.18	21
181.208.245.97	181.208.245.97	20
179.4.120.29	179.4.120.29	19
192.168.1.26	192.168.1.26	19
181.130.85.19	181.130.85.19	19
189.114.3.213	189.114.3.213	18

Application Usage By Category

As part of the traffic classification process, the FortiGate identifies and categorizes the applications crossing the network into different categories based on the number of sessions and bandwidth. This data complements the granular application threat data and provides a more complete summary of the types of applications in use on the network.

Application Usage By Category



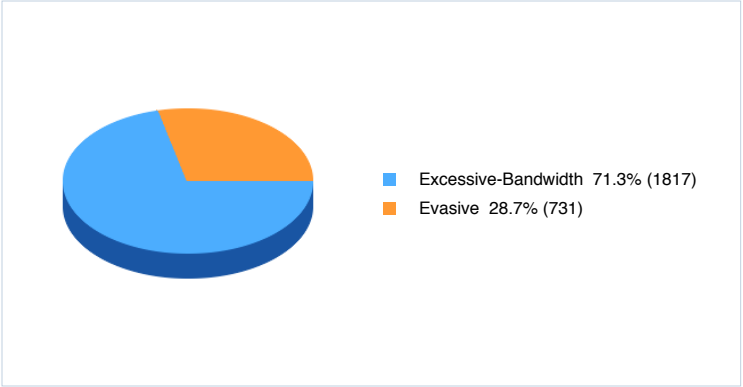
Top 30 Application Category

Application Category	Bandwidth
Web.Others	556.30 MB
Video/Audio	134.82 MB
Network.Service	128.53 MB
Collaboration	2.72 MB
General.Interest	2.41 MB
Storage.Backup	2.12 MB
File.Sharing	2.12 MB
Social.Media	1.43 MB
Email	743.87 KB
IM	112.87 KB
Update	99.11 KB
Remote.Access	65.12 KB

Applications Detected by Risk Behavior

Modern security organizations need increasingly complex security processes in place to handle the myriad applications in use on the network and in the data center. The problem is determining which applications in your environment are most likely to cause harm. The following charts provide a breakdown of the high risk applications identified on the network. It has been determined by FortiGuard Labs that these applications represent possible vectors for data compromise, network intrusion, or a reduction in network performance.

Breakdown of Risk Applications



Number of Applications by Risk Behavior

Risk	Number of Applications
Evasive	731
Excessive-Bandwidth	1817
Other Applications	15097

High Risk Applications

Risk	Application Name	Category	Technology	Bandwidth	Sessions
Evasive	Twitter	Social.Media	Browser-Based	1.04 MB	562
Evasive	SMTPS	Email	Network-Protocol	550.96 KB	111
Evasive	Dropbox	File.Sharing	Browser-Based	2.06 MB	38
Evasive	IMAPS	Email	Network-Protocol	87.72 KB	14
Evasive	RTMP	Network.Service	Network-Protocol	11.55 KB	2
Evasive	Gotomeeting	Collaboration	Browser-Based	14.40 KB	2
Evasive	Stumbleupon.Toolbar	General.Interest	Browser-Based	1.57 KB	1
Evasive	Jabber	IM	Client-Server	112.87 KB	1
Excessive-Bandwidth	Fortiguard.Search	General.Interest	Browser-Based	1.98 MB	1.11 K
Excessive-Bandwidth	iCloud	Storage.Backup	Browser-Based	2.03 MB	181
Excessive-Bandwidth	Youtube	Video/Audio	Browser-Based	2.25 MB	135
Excessive-Bandwidth	iTunes	Video/Audio	Client-Server	8.17 MB	126
Excessive-Bandwidth	IP.Multicast	Network.Service	Network-Protocol	36.06 KB	60
Excessive-Bandwidth	HTTP.Video	Web.Others	Browser-Based	147.49 MB	54
Excessive-Bandwidth	Youtube_HD.Streaming	Video/Audio	Browser-Based	123.07 MB	40
Excessive-Bandwidth	Akamai	File.Sharing	Browser-Based	4.91 KB	32
Excessive-Bandwidth	iTunes_Store	Video/Audio	Browser-Based	955.83 KB	25
Excessive-Bandwidth	Google.Plus	Social.Media	Browser-Based	4.67 KB	19
Excessive-Bandwidth	Cienradios	Video/Audio	Browser-Based	346.13 KB	13
Excessive-Bandwidth	HTTP.Audio	Web.Others	Browser-Based	18.93 MB	10

Key Applications Crossing The Network

This part of the PoC Security Report offers a summary of the key applications crossing the network based on the amount of bandwidth they are using and then sorted into different application types. It provides a high level view of the types of application that are used most commonly across the network.

Key Applications Crossing The Network

Application	Category	Sessions	Bandwidth
HTTP.BROWSER_Safari	Web.Others	2138	341.39 MB
HTTP.Video	Web.Others	54	147.49 MB
SSL	Network.Service	7575	127.22 MB
Youtube_HD.Streaming	Video/Audio	40	123.07 MB
HTTP.BROWSER	Web.Others	239	27.13 MB
HTTP.Audio	Web.Others	10	18.93 MB
HTTP.Flash	Web.Others	3	16.86 MB
Web Management(HTTPS)		108	13.03 MB
iTunes	Video/Audio	126	8.17 MB
HTTP.BROWSER_Firefox	Web.Others	115	3.52 MB
Zoho	Collaboration	73	2.69 MB
Youtube	Video/Audio	135	2.25 MB
Dropbox	File.Sharing	38	2.06 MB
iCloud	Storage.Backup	181	2.03 MB
Fortiguard.Search	General.Interest	1109	1.98 MB
Twitter	Social.Media	562	1.04 MB
iTunes_Store	Video/Audio	25	955.83 KB
DNS	Network.Service	3881	708.52 KB
SMTPS	Email	111	550.96 KB
Console Management(SSH)		3	519.40 KB
Geckoboard	Web.Others	12	515.99 KB
Salesforce	General.Interest	12	411.04 KB
Facebook	Social.Media	26	372.03 KB
Cienradios	Video/Audio	13	346.13 KB
ICMP	Network.Service	685	287.19 KB
HTTP.BROWSER_IE	Web.Others	18	268.43 KB
OCSP	Network.Service	96	210.62 KB
HTTP.PDF	Web.Others	1	198.32 KB
Jabber	IM	1	112.87 KB
Gmail	Email	8	105.19 KB

Applications Running Over HTTP

This section provides an overview of applications crossing the network that use HTTP. Software updates, error reporting or help guides are used by different business applications as a means of improving the overall user experience. Social networks, streaming video or audio, file sharing are among the most common non-business applications that use HTTP. Assessing the number and type of applications that use HTTP provides a critical part of developing an efficient network security strategy.

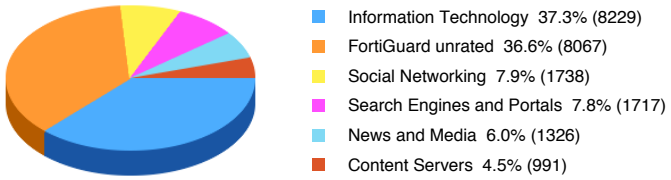
Applications Running Over HTTP

Application	Sessions	Bandwidth
HTTP.BROWSER_Safari	2137	341.39 MB
HTTP.Video	54	147.49 MB
SSL	7532	125.90 MB
Youtube_HD.Streaming	40	123.07 MB
HTTP.BROWSER	238	27.13 MB
HTTP.Audio	10	18.93 MB
HTTP.Flash	3	16.86 MB
Web Management(HTTPS)	108	13.03 MB
iTunes	126	8.17 MB
HTTP.BROWSER_Firefox	115	3.52 MB
Youtube	128	2.20 MB
Zoho	49	2.13 MB
iCloud	181	2.03 MB
Dropbox	37	1.85 MB
Twitter	554	984.91 KB
iTunes_Store	25	955.83 KB
Zoho	24	555.74 KB
Geckoboard	12	515.99 KB
Salesforce	12	411.04 KB
Facebook	20	349.85 KB
Cienradios	13	346.13 KB
HTTP.BROWSER_IE	18	268.43 KB
OCSP	96	210.62 KB
Dropbox	1	204.93 KB
HTTP.PDF	1	198.32 KB

Top Web Categories Visited By Network Users

User browsing habits can not only be indicative of inefficient use of corporate resources, but can also indicate an inefficient optimization of web filtering policies. It can also give some insight into the general web browsing habits of corporate users and assist in defining corporate compliance guidelines. This chart details web categories by the number of times URLs within those categories were requested and by the number of bandwidth used.

Top Web Categories



Top Web Sites Visited By Network Users

Category Description	Sessions	Bandwidth
Information Technology	8229	6.55 MB
FortiGuard unrated	8067	615.36 MB
Social Networking	1738	967.75 KB
Search Engines and Portals	1717	2.98 MB
News and Media	1326	3.95 MB
Content Servers	991	711.89 KB
Streaming Media and Download	865	1.29 MB
File Sharing and Storage	647	989.90 KB
Advertising	547	681.68 KB
Meaningless Content	369	158.03 KB
Internet Radio and TV	182	75.02 KB
Web-based Email	75	177.04 KB
Business	74	57.34 KB
Reference	72	92.86 KB
Web-based Applications	55	36.51 KB
Travel	35	27.03 KB
Internet Telephony	26	82.00 KB
Finance and Banking	22	44.47 KB
Illegal or Unethical	21	10.46 KB
Web Hosting	16	3.09 KB

Top Web Sites Visited By Network Users

Identifying and managing the top URLs visited by network users provides greater visibility and control, and subsequently, better network security. By leveraging Fortinet threat prevention, application control and URL filter technologies, the volume of web sites by category can be reviewed and strategies put in place to prevent users accessing sites considered to be a risk to overall network security.

Top Visited Hostname

Domain	Category Description	Visits
fortinet.com	Information Technology	4703
twitter.com	Social Networking	1543
mozilla.org	Information Technology	1081
twitter.com	FortiGuard unrated	1025
continental.com.ar	FortiGuard unrated	972
mzstatic.com	FortiGuard unrated	926
youtube.com	FortiGuard unrated	759
mzstatic.com	Information Technology	756
youtube.com	Streaming Media and Download	742
google.com	Search Engines and Portals	736
googlevideo.com	Search Engines and Portals	713
continental.com.ar	News and Media	690
googlevideo.com	FortiGuard unrated	547
ytimg.com	FortiGuard unrated	462
ytimg.com	Content Servers	440
qaotic.net	FortiGuard unrated	426
icloud.com	File Sharing and Storage	380
clarin.com	News and Media	361
qaotic.net	Meaningless Content	361
clanacion.com.ar	Content Servers	318

Top Destination Countries By Browsing Time

The following chart shows the distribution of web traffic according to the destination country. This chart offers the possibility to the network administrator to analyze which countries web sites are visited for longer time. The administrator can then decide to create security policy based on Geo-location.

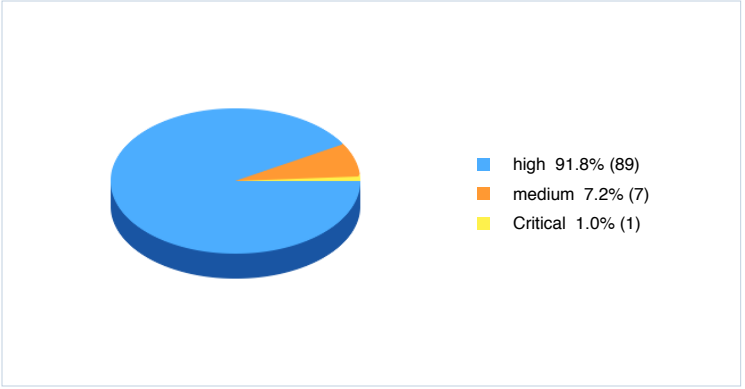
Top destination Countries by Browsing Time

Country	Bandwidth	Traffic Received	Traffic Sent
US	476.59 MB	74.86 MB	401.72 MB
AR	337.50 MB	1.92 MB	335.57 MB
Reserved	23.64 MB	8.75 MB	14.89 MB
CA	16.15 MB	366.92 KB	15.78 MB
CO	8.65 MB	217.05 KB	8.43 MB
PE	1.55 MB	478.38 KB	1.08 MB
DE	1.05 MB	93.62 KB	960.88 KB
IE	1.01 MB	416.10 KB	598.58 KB
SG	938.68 KB	271.05 KB	667.63 KB
NL	894.53 KB	52.86 KB	841.66 KB
UY	590.99 KB	11.56 KB	579.42 KB
GB	524.54 KB	258.17 KB	266.37 KB
FR	479.95 KB	27.10 KB	452.86 KB
ES	224.80 KB	9.35 KB	215.46 KB
SK	218.63 KB	3.01 KB	215.63 KB

Top Threats Crossing The Network

By individually reviewing both the applications and traffic flows crossing the network, threat vector identification and prevention becomes easier. Threat prevention technologies filter the total number of applications and traffic crossing the network down to those applications or packets that pose a potential risk, picking up threat vectors such as spyware, application vulnerabilities or viruses. The result is improved overall network performance and lower network latency.

Top Threat Vectors Crossing The Network



Top Critical Threat Vectors Crossing The Network

Attack Name	Reference	Total Num
Cisco.IOS.HTTP.Remote.Command.Execution	http://www.fortinet.com/ids/VID30478	1

Top High Threat Vectors Crossing The Network

Attack Name	Reference	Total Num
Cisco.CSCdv50135.Telnet.Buffer.Overflow	http://www.fortinet.com/ids/VID32370	89

Top Medium Threat Vectors Crossing The Network

Attack Name	Reference	Total Num
Cisco.514.UDP.Flood.DoS	http://www.fortinet.com/ids/VID32375	3
Cisco.600.Series.Web.Administration.DoS	http://www.fortinet.com/ids/VID32374	1
Cisco.UTF.Encoding.IDS.Bypass	http://www.fortinet.com/ids/VID32373	1
Cisco.CatOS.CiscoView.HTTP.Server.Buffer.Overflow	http://www.fortinet.com/ids/VID32372	1
Cisco.IOS.HTTP.Server.Query.DoS	http://www.fortinet.com/ids/VID32376	1

Top Low Threat Vectors Crossing The Network

No matching log data for this report

Top Info Threat Vectors Crossing The Network

No matching log data for this report

Top 20 Viruses Crossing The Network

As the FortiGate scans the network, it provides information about the viruses that are crossing the network. The Fortigate is able to apply different strategies in order to detect malware: - Signatures: Fortinet's Compact Pattern Recognition Language (CPRL) - Heuristics: These are applied to: * file structure; * API call. The FortiGate's antivirus engine provides two main capabilities: Decompression allows embedded files to be extracted; Emulation allows the hidden layers of malicious file of be extracted.

Top 20 Virus By Name

Virus Name	Occurrences
EICAR_TEST_FILE	24

Top Virus Victims

This counter provides information about which network users are more prone to infection from viruses. This enables direct identification of the host(s) that are creating sources of malicious traffic on the network. The following chart displays the counter of the number of viruses per end user.

Top 20 Virus Victim

Virus Victim	Occurrences
192.168.1.44	17
192.168.1.110	7

Application Virus Discovered

Day	Malware
2013-12-13	17
2013-12-16	7

Appendix A

Devices: FGT60C3G12047125[root]